МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
БОРИСОГЛЕБСКИЙ ФИЛИАЛ
(БФ ФГБОУ ВО «ВГУ»)

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
Теоретические основы информатики

Методические указания для обучающихся по освоению дисциплины

Приступая к изучению учебной дисциплины, прежде всего обучающиеся должны ознакомиться с учебной программой дисциплины. Электронный вариант рабочей программы размещён на сайте БФ ВГУ.

Знание основных положений, отраженных в рабочей программе дисциплины, поможет обучающимся ориентироваться в изучаемом курсе, осознавать место и роль изучаемой дисциплины в подготовке будущего педагога, строить свою работу в соответствии с требованиями, заложенными в программе.

Основными формами контактной работы по дисциплине являются лекции, практические и лабораторные занятия, посещение которых обязательно для всех студентов (кроме студентов, обучающихся по индивидуальному плану).

В ходе лекционных занятий следует не только слушать излагаемый материал и кратко его конспектировать, но очень важно участвовать в анализе примеров, предлагаемых преподавателем, в рассмотрении и решении проблемных вопросов, выносимых на обсуждение. Необходимо критически осмысливать предлагаемый материал, задавать вопросы как уточняющего характера, помогающие уяснить отдельные излагаемые положения, так и вопросы продуктивного типа, направленные на расширение и углубление сведений по изучаемой теме, на выявление недостаточно освещенных вопросов, слабых мест в аргументации и т.п.

Не следует дословно записывать лекцию, лучше попытаться понять логику изложения и выделить наиболее важные положения лекции в виде опорного конспекта. Рекомендуется использовать различные формы выделения наиболее сложного, нового, непонятного материала, который требует дополнительной проработки: можно пометить его знаком вопроса (или записать на полях сам вопрос), цветом, размером букв и т.п. – это поможет быстро найти материал, вызвавший трудности, и в конце лекции (или сразу же, попутно) задать вопрос преподавателю (не следует оставлять непонятый материал без дополнительной проработки, без него иногда бывает невозможно понять последующие темы). Материал уже знакомый или понятный нуждается в меньшей детализации – это поможет сэкономить усилия во время конспектирования.

На практических занятиях необходимо активно участвовать в решении предлагаемых задач, начиная уже с этапа анализа условия и поиска путей решения. Студенту, вызванному для решения задачи к доске, следует подробно комментировать ход решения задачи, а стальным студентам — выполнять основные этапы решения предложенной задачи самостоятельно, но при этом контролируя ход решения на доске. При возникновении проблем с решением какой-либо задачи, рекомендуется сразу же задать вопрос преподавателю: непонимание, возникшее, при решении одной задачи, может помешать решать последующие.

При выполнении лабораторных работ следует пользоваться конспектом лекций и тетрадью с решением задач с практических занятий. Решения оформляются с использованием текстового процессора (например, MS Word) и содержат, помимо ответов, подробное решение каждой задачи. Также при решении задач рекомендуется активно использовать для проведения необходимых расчётов и вычислений возможности табличных процессоров (например, MS Excel) и (по желанию) известных обучающимся языков программирования.

При подготовке к промежуточной аттестации необходимо повторить пройденный материал в соответствии с учебной программой, примерным перечнем вопросов, выносящихся на зачет. Рекомендуется использовать конспекты лекций и источники, перечисленные в списке литературы в рабочей программе дисциплины, а также ресурсы электронно-библиотечных систем. Необходимо обратить особое внимание на темы учебных занятий, пропущенных по разным причинам. При необходимости можно обратиться за консультацией и методической помощью к преподавателю.

План лекционных занятий

Тема №1. Предмет теоретической информатики

- Информатика как наука. Структура и место в системе наук.
- Теоретическая информатика. Основные понятия теоретической информатики.

Тема №2. Теория информации

- Теория информации Шеннона.
- Принципы получения, хранения, обработки и использования информации.
- Энтропия и информация

Тема №3. Теория кодирования

- Задача кодирования. Виды кодирования. Побуквенное кодирование.
- Первая теорема Шеннона. Неравномерное и равномерное двоичное кодирование.
- Оптимальные коды. Префиксные коды. Код Хаффмана. Код Шеннона-Фано. Блочное кодирование.
- Вторая теорема Шеннона. Помехоустойчивые коды. Систематические коды. Коды Хэмминга.

Тема №4. Теория распознавания образов

- Проблема распознавания. Постановка задачи распознавания. Общая характеристика задач распознавания и их типы.
- Математическая теория распознавания образов. Подходы к задаче распознавания.
- Геометрические процедуры распознавания. Линейные разделяющие функции и поверхности решений.

Тема №5. Математическая кибернетика

- Информация и управление.
- Система как объект исследования в кибернетике.
- Математические аспекты кибернетики.

Методические материалы к практическим занятиям по теме «Теория кодирования»

Теория кодирования информации является одним из разделов теоретической информатики. К её основным задачам относятся следующие:

- разработка принципов *наиболее экономичного* кодирования информации;
- согласование параметров передаваемой информации с особенностями канала связи;
- разработка приемов, обеспечивающих *надёжность* передачи информации по каналам связи, то есть отсутствие потерь информации.

Для представления дискретной информации используется некоторый *алфавит*. Однозначное соответствие между информацией и алфавитом отсутствует. Другими словами, одна и та же информация может быть представлена посредством различных алфавитов. Поэтому возникает проблема перехода от одного алфавита к другому, причем такое преобразование не должно приводить к потере информации. Условимся называть алфавит, с помощью которого представляется информация до преобразования, *первичным*; алфавит конечного представления — *вторичным*.

Введем ряд определений:

Код — правило, описывающее соответствие знаков или их сочетаний одного алфавита знакам или их сочетаниям другого алфавита, а также знаки вторичного алфавита, используемые для представления знаков или их сочетаний первичного алфавита.

Кодирование — перевод информации, представленной посредством первичного алфавита, в последовательность кодов.

Декодирование — операция, обратная кодированию, то есть восстановление информации в первичном алфавите по полученной последовательности кодов.

Операции кодирования и декодирования называются *обратимыми*, если их последовательное применение обеспечивает возврат к исходной информации без каких-либо её потерь.

Виды кодирования

В зависимости от целей кодирования, различают следующие его виды:

1) *Кодирование по образцу* — каждый знак дискретного сигнала представляется знаком или набором знаков того алфавита, в котором выполняется кодирование. Используется, в частности, всякий раз для ввода информации в компьютер для ее внутреннего представления.
2) *Эффективное* (оптимальное) кодирование — для устранения избыточности данных путем снижения среднего числа символов кодового алфавита для представления одного исходного символа. Именно этот вид кодирования используется для сжатия.
3) *Помехоустойчивое* (помехозащитное) кодирование — для обеспечения заданной достоверности в случае, когда на сигнал накладывается помеха. Используется для защиты от помех при передаче информации по каналам связи.
4) *Криптографическое* кодирование (шифрование) — используется, когда нужно защитить информацию от несанкционированного доступа.

Приведём математическую постановку задачи кодирования.

Пусть первичный алфавит A содержит N знаков со средней информацией на знак, определённой с учетом вероятностей их появления, $I_1(A)$ (нижний индекс отражает то обстоятельство, что рассматривается первое приближение, а буква в скобках указывает алфавит). Вторичный алфавит B пусть содержит M знаков со средней информационной ёмкостью $I_1(B)$. Пусть также исходное сообщение, представленное в первичном алфавите, содержит n знаков, а закодированное сообщение — m знаков. Если исходное сообщение содержит $I(A)$ информации, а закодированное — $I(B)$, то условие обратимости кодирования, то есть *неисчезновения* информации при кодировании, очевидно, может быть записано следующим образом:

$$I(A) \le I(B).$$

Смысл неравенства в том, что *операция обратимого кодирования может увеличить количество формальной информации в сообщении, но не может его уменьшить*. Каждая из величин в данном неравенстве может быть заменена произведением числа знаков на среднюю информационную емкость знака:

$$I_1(A) \le \frac{m}{n} I_1(B), \quad I_1(A) = -\sum_{i=1}^{N} p_i \log_2 p_i.$$

Отношение $K(B) = m/n$, очевидно, характеризует *среднее число знаков вторичного алфавита, которое приходится использовать для кодирования одного знака первичного алфавита* — будем называть его *длиной кода*.

В частном случае, когда появление любых знаков вторичного алфавита равновероятно, согласно формуле Хартли $I_1(B) = \log_2 M$, и тогда

$$\frac{I_1(A)}{\log_2 M} \le K(B).$$

Методические материалы к лекционным и практическим занятиям по теме «Эффективное кодирование»

Используя обозначения для математической постановки задачи кодирования, введем в рассмотрение новую величину — *относительную избыточность кода* (Q):

$$Q = 1 - \frac{I(A)}{I(B)} = 1 - \frac{I_1(A)}{K(B)I_1(B)}.$$

Данная величина показывает, насколько операция кодирования увеличила длину исходного сообщения. Очевидно, чем меньше Q (то есть чем ближе она к *0* или, что тоже, $I(B)$ ближе к $I(A)$), тем более выгодным оказывается код и более *эффективной* операция кодирования.

Отметим, что на практике для оценки средней длины кода пользуются формулой из теории вероятностей:

$$K(B) = \sum_{i=1}^{N} p_i k_i,$$

где k_i — длина кода для символа с частотой p_i.

Для теории связи важнейшее значение имеет следующая теорема.

Первая теорема Шеннона о передаче информации, которая называется также *основной теоремой о кодировании при отсутствии помех*, формулируется следующим образом:

При отсутствии помех передачи всегда возможен такой вариант кодирования сообщения, при котором избыточность кода будет сколь угодно близкой к нулю.

Важно, что теорема открывает принципиальную возможность оптимального кодирования. Однако необходимо сознавать, что из теоремы никоим образом не следует, как такое кодирование осуществить практически.

С практической точки зрения наиболее просто реализуемый вариант – ситуация, когда $M = 2$, то есть для представления кодов в линии связи используется лишь два типа сигналов. Подобное кодирование называется *двоичным*. Знаки двоичного алфавита принято обозначать «*0*» и «*1*», но нужно воспринимать их как буквы, а не цифры. Удобство двоичных кодов и в том, что при равных длительностях и вероятностях каждый элементарный сигнал (*0* или *1*) несет в себе 1 бит информации ($\log_2 M = 1$); тогда

$$I_1(A) = K(2),$$

и первая теорема Шеннона получает следующую интерпретацию:

При отсутствии помех передачи средняя длина двоичного кода может быть сколь угодно близкой к средней информации, приходящейся на знак первичного алфавита.

Тогда формула избыточности для двоичного кодирования дает:

$$Q = 1 - \frac{I_1(A)}{K(2)}.$$

Итак, первая теорема Шеннона открывает возможность эффективного кодирования. Рассмотрим подходы к построению эффективных кодов.

Согласно теории информации Шеннона, количество получаемой с сообщением информации тем больше, чем неожиданнее данное сообщение. Этот тезис использован при эффективном кодировании кодами переменной длины: исходные символы, имеющие большую вероятность (или частоту), имеют код меньшей длины и наоборот.

Таким образом, эффективное кодирование предполагает использование кодов разной длины — коротких для часто встречающихся символов и более длинных — для редких. Но в таком случае возникает проблема отделения кодов разных символов друг от друга — нужно знать, когда закончился один код и начался другой.

Для этого можно вести специальный *код-разделитель* (например, в коде Морзе для этого используется пауза), но это понизит эффективность кода, так как увеличит его длину. Однако очевидно, что эффективность данного способа кодирования невелика.

Легко заметить, что одной из причин этого является присутствие в коде каждого символа «лишних» бит — разделителя, не несущего информации.

Можно найти такой вариант кодирования сообщения, при котором последующее выделение из него каждого отдельного знака (то есть декодирование) оказывается однозначным без специальных указателей разделения знаков. Наиболее простыми и употребимыми кодами такого типа являются так называемые *префиксные коды*, которые удовлетворяют следующему условию (*условие Фано*):

Неравномерный код может быть однозначно декодирован, если никакой из кодов не совпадает с началом какого-либо иного более длинного кода.

Например, если имеется код *110*, то уже не могут использоваться коды *1*, *11*, *1101*, *110101* и пр. Если условие Фано выполняется, то при прочтении (расшифровке) закодированного сообщения путём сопоставления со списком кодов всегда можно точно указать, где заканчивается один код и начинается другой.

Таким образом, использование префиксного кодирования позволяет делать сообщение более коротким, поскольку нет необходимости передавать разделители знаков. Однако условие Фано не устанавливает способа формирования префиксного кода и, в частности, наилучшего из возможных.

Метод Шеннона-Фано

Один из первых методов построения префиксных кодов.

Для построения кода методом Шеннона-Фано можно использовать таблицу или кодовое дерево. Опишем процесс построения кода с помощью таблицы.

Исходное множество символов упорядочивается по невозрастанию частот (вероятностей) их встречаемости в тексте, и выполняются следующие шаги.

1. Список символов делится на две части так, чтобы суммы частот обеих частей были точно или примерно равны.
2. Кодовым комбинациям первой части дописываются единицы, второй части — нули.
3. Если первая часть содержит только один символ, работа с ней заканчивается, и осуществляется переход к шагу 4, иначе — переход к шагу 1 и алгоритм применяется к первой части как к целому алфавиту.
4. Если вторая часть содержит только один символ, работа с ней заканчивается, и осуществляется переход к шагу 5, иначе — переход к шагу 1 и алгоритм применяется ко второй части как к целому алфавиту.
5. Если оставшийся список пуст (в каждой группе по одному символу) — код построен, работа алгоритма заканчивается. Иначе — выполняется шаг 1 для оставшейся группы символов.

Рассмотрим пример.

Пусть даны символы a, b, c, d с частотами $f_a = 0.3$; $f_b = 0.4$; $f_c = 0.1$; $f_d = 0.2$. Построим эффективный код методом Шеннона-Фано.

Процесс построения кода представлен в таблице.

<table>
<tr><th>Исходные символы s</th><th>Частоты f_s</th><th>I</th><th>II</th><th>III</th><th>Код</th></tr>
<tr><td>b</td><td>0.4</td><td>1</td><td></td><td></td><td>1</td></tr>
<tr><td>a</td><td>0.3</td><td rowspan="3">0</td><td>1</td><td></td><td>01</td></tr>
<tr><td>d</td><td>0.2</td><td rowspan="2">0</td><td>1</td><td>001</td></tr>
<tr><td>c</td><td>0.1</td><td>0</td><td>000</td></tr>
</table>

Метод Хаффмана

Метод кодирования Хаффмана относится к префиксным кодам и является неулучшаемым, то есть невозможно построить префиксный код символьного кодирования с большей эффективностью.

Опишем алгоритм кодирования Хаффмана.

Исходное множество символов упорядочивается по невозрастанию частот (вероятностей) их встречаемости в тексте, и выполняются следующие шаги.

1. Объединение частот:
   - две последние (самые маленькие) частоты складываются, а соответствующие символы исключаются из списка;
   - оставшийся после исключения символов список пополняется суммой частот и вновь упорядочивается;
   - предыдущие шаги повторяются до тех пор, пока не получится единица в результате суммирования и список не уменьшится до одного символа.
2. Построение кодового дерева:
   - строится двоичное кодовое дерево: корнем его является вершина, равная 1; остальные вершины соответствуют либо суммарным, либо исходным частотам, причём для каждой вершины левая подчинённая вершина соответствует большему слагаемому, а правая — меньшему;
   - рёбра дерева кодируются: каждое левое кодируется единицей, каждое правое — нулем.
3. Формирование кода: для получения кодов листьев (исходных кодируемых символов) продвигаются от корня к нужной вершине и записывают веса проходимых ребер.

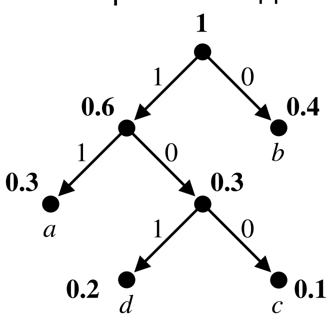
Рассмотрим пример.

Пусть даны символы a, b, c, d с частотами $f_a = 0.3$; $f_b = 0.4$; $f_c = 0.1$; $f_d = 0.2$. Построим эффективный код методом Хаффмана.

1. Объединение частот.

Исходные символы s	Частоты f_s	Этапы объединения		
		первый	второй	третий
b	0.4	0.4	0.6	1
a	0.3	0.3	0.4	
d	0.2	0.3		
c	0.1			

2. Построение кодового дерева.



3. Формирование кода.

b: 0;
a: 11;
d: 101;
c: 100.

Блочное двоичное кодирование

При алфавитном кодировании наилучший результат (наименьшая избыточность) может быть получен при кодировании по методу Хаффмана – для русского алфавита избыточность составит менее *1%*. При этом известно, что код Хаффмана улучшить невозможно.

Для повышения эффективности кодирования от алфавитных методов переходят к *блочному кодированию*. При алфавитном кодировании передаваемое сообщение представляет собой последовательность кодов отдельных знаков первичного алфавита. Однако возможны варианты кодирования, при которых кодовый знак относится сразу к нескольким буквам первичного алфавита (будем называть такую комбинацию *блоком*) или даже к целому слову первичного языка. Кодирование блоков понижает избыточность.

Например, пусть даны символы a и b с частотами, соответственно, 0.9 и 0.1. Построим эффективный код методом Хаффмана для блоков из двух символов.

Сформируем список возможных блоков и их частот (при этом частоту блока будем рассчитывать как произведение частот символов, входящих в блок) и построим код по методу Хаффмана. Тогда имеем:

Блоки	Частоты	Код
aa	0.81	1
ab	0.09	00
ba	0.09	011
bb	0.01	010

Определим эффективность построенного кода. Для этого рассчитаем сначала показатель эффективности для блока символов по формуле:

$$K_2(2) = 0.81*1 + 0.09*2 + 0.09*3 + 0.01*3 = 1.28.$$

Поскольку в блоке 2 символа, то для одного символа:

$$K(2) = K_2(2)/2 = 1.28/2 = 0.64.$$

При посимвольном кодировании для эффективного кода потребуется по одному двоичному разряду. Таким образом, при блочном кодировании выигрыш составил $1-0.64=0.36$ двоичных разрядов на один кодируемый символ в среднем.

Эффективность блочного кодирования тем выше, чем больше символов включается в блок.

Однако, несмотря на кажущиеся преимущества, применение блочного и словесного метода кодирования имеет свои недостатки. Во-первых, необходимо хранить огромную кодовую таблицу и постоянно к ней обращаться при кодировании и декодировании, что замедлит работу и потребует значительных ресурсов памяти. Во-вторых, помимо основных слов, разговорный язык содержит много производных от них, например, падежи существительных в русском языке или глагольные формы в английском. При кодировании данным способом реальных словарей, им всем нужно присвоить свои коды, что приведет к увеличению кодовой таблицы еще в несколько раз. В-третьих, возникает проблема согласования (стандартизации) этих громадных таблиц, что непросто. Наконец, в-четвертых, алфавитное кодирование имеет то преимущество, что буквами можно закодировать любое слово, а при кодировании слов можно использовать только имеющийся словарный запас. По указанным причинам на практике, как правило, применяется алфавитное кодирование.

Методические материалы к лекционным и практическим занятиям по теме «Помехоустойчивое кодирование. Вторая теорема Шеннона. Код Хэмминга»

Под *помехой* понимается любое воздействие, накладывающееся на полезный сигнал и затрудняющее его прием.

Кодирование, устойчивое к помехам, должно осуществляться так, чтобы сигнал, соответствующий принятой последовательности символов, после воздействия на него предполагаемой в канале помехи, оставался ближе к сигналу, соответствующему конкретной переданной последовательности символов, чем к сигналам, соответствующим другим возможным последовательностям.

Это достигается ценой введения при кодировании избыточности, которая позволяет так выбрать передаваемые последовательности символов, чтобы они удовлетворяли дополнительным условиям, проверка которых на приемной стороне дает возможность обнаружить и исправить ошибки.

Коды, обладающие таким свойством, получили название *помехоустойчивых.* Они используются как для исправления ошибок (корректирующие коды), так и для их обнаружения.

Теория помехоустойчивого кодирования базируется на результатах исследований, проведенных Шенноном и сформулированных им в виде *основной теоремы для дискретного канала с шумом* (**Вторая теорема Шеннона**): *при любой скорости передачи двоичных символов меньшей, чем пропускная способность канала,* *существует такой код, при котором вероятность ошибочного декодирования будет сколь угодно мала*.

Как видно, в теореме не затрагивается вопрос о путях построения кода, обеспечивающего указанную идеальную передачу. Тем не менее, значение ее огромно, поскольку, обосновав принципиальную возможность такого кодирования, она мобилизовала усилия ученых на разработку конкретных кодов.

Очевидно, что при взаимно независимых ошибках наиболее вероятен переход в кодовую комбинацию, отличающуюся от данной в наименьшем числе символов.

Степень различия любых двух кодовых комбинаций характеризуется *расстоянием по Хэммингу* или *кодовым расстоянием*. Оно выражается числом символов, в которых комбинации отличаются, и обозначается d.

Чтобы рассчитать кодовое расстояние между двумя комбинациями двоичного кода, достаточно подсчитать число единиц в сумме этих комбинаций по модулю 2.

Декодирование после приема может производиться таким образом, что принятая кодовая комбинация отождествляется с той разрешенной, которая отличается от полученной в наименьшем числе символов. Такое декодирование называется декодированием по *методу максимального правдоподобия*.

В общем случае при необходимости обнаруживать ошибки кратности r минимальное кодовое расстояние между разрешенными кодами:

$$d \geq r+1.$$

Для возможности исправления ошибок кратности s и менее кодовое расстояние должно удовлетворять соотношению:

$$d \geq 2s+1.$$

Нетрудно убедиться в том, что для исправления всех ошибок кратности s и менее и одновременного обнаружения всех ошибок кратности r ($r \geq s$) и менее минимальное кодовое расстояние:

$$d \geq r+s+1.$$

Код Хэмминга

Код Хэмминга представляет собой один из важнейших классов помехоустойчивых кодов, нашедших широкое применение на практике и имеющих простой и удобный для технической реализации алгоритм обнаружения и исправления одиночной ошибки.

Предположим, необходимо исправить одиночную ошибку двоичного кода. Такой код состоит из $n_и$ символов, несущих информацию, и n_k контрольных (избыточных) символов. Всего символов в коде

$$n = n_и + n_к.$$

При передаче кода может быть искажен любой информационный символ. Однако может быть и такой вариант, что ни один из символов не будет искажен, то есть если всего в коде n символов, то с помощью контрольных символов, входящих в это число, должно быть создано такое число комбинаций $2^{n_к}$, чтобы свободно различить $n+1$ вариант.

Поэтому $n_к$ должно удовлетворять неравенству

$$2^{n_к} \geq n+1.$$

Тогда

$$2^n = 2^{n_к+n_и} = 2^{n_к} \cdot 2^{n_и},$$

$$2^n \geq (n+1) \cdot 2^{n_и},$$

где 2^n — полное число комбинаций кода.

Следовательно, число информационных символов кода, обнаруживающего и корректирующего одиночную ошибку, может быть оценено из соотношения:

$$2^{n_и} \le \frac{2^n}{(n+1)}.$$

Для вычисления основных параметров кода Хэмминга задается количество либо информационных символов, либо информационных комбинаций $N = 2^{n_и}$. При помощи приведённых выше формул вычисляют n и n_k.

Зная основные параметры корректирующего кода, определяют, какие позиции сигналов будут рабочими, а какие — контрольными. Практика показала, что номера контрольных символов удобно выбирать по закону 2^i, где $i = 0, 1, 2, 3, \dots$. Номера контрольных символов в этом случае равны 1, 2, 4, 8,….

0001	a_1
0010	a_2
0011	a_3
0100	a_4
0101	a_5
0110	a_6
0111	a_7
1000	a_8
1001	a_9
1010	a_{10}
1011	a_{11}

Затем определяют значения контрольных коэффициентов (0 или 1), руководствуясь следующим правилом: *сумма единиц на проверочных позициях должна быть чётной.* Если эта сумма чётна — значение контрольного коэффициента ноль, в противном случае — единица.

Проверочные позиции выбирают следующим образом. Составляют таблицу для ряда натуральных чисел в двоичном коде. Число её строк $n = n_k + n_и$. Первой строке этой таблицы соответствует проверочный коэффициент a_1, второй a_2 и т.д.

Пример таблицы для определения проверочных позиций при $n = 11$ приведён рядом.

Проверочные позиции выявляют, выписывая коэффициенты по следующему принципу: в первую проверку входят коэффициенты, которые содержат единицу в младшем разряде ($a_1, a_3, a_5, a_7, a_9, a_{11}$ и т.д.); во вторую — во втором разряде ($a_2, a_3, a_6, a_7, a_{10}, a_{11}$ и т.д.); в третью — в третьем разряде и т.д.

Пример построения кода Хэмминга

Позиция символов	Кодовое слово	
	Макет	Итог
1	K_1	0
2	K_2	1
3	0	0
4	K_3	0
5	1	1
6	0	0
7	1	1

Пусть необходимо построить макет кода Хэмминга и определить значения корректирующих разрядов для кодовой комбинации ($n_и = 4$) 0101.

Согласно полученной выше формуле минимальное число контрольных символов $n_к = 3$, при этом $n = 7$. Контрольные коэффициенты будут расположены на позициях 1, 2, 4. Составим макет корректирующего кода и запишем его во вторую колонку таблицы.

Пользуясь правилом о чётности элементов в проверочных позициях, определим значения коэффициентов K_1, K_2 и K_3.

Первая проверка: сумма $П_1 + П_3 + П_5 + П_7$ должна быть четной, а сумма $K_1 + 0 + 1 + 1$ будет четной при $K_1 = 0$.

Вторая проверка: сумма $П_2 + П_3 + П_6 + П_7$ должна быть четной, а сумма $K_2 + 0 + 0 + 1$ будет четной при $K_2 = 1$.

Третья проверка: сумма $\Pi_4+\Pi_5+\Pi_6+\Pi_7$ должна быть четной, а сумма $K_3+1+0+1$ будет четной при $K_3=0$.

Окончательное значение искомой комбинации корректирующего кода записываем в третью колонку таблицы.

Обнаружение и исправление ошибок в коде Хэмминга

Предположим, в канале связи под действием помех произошло искажение и вместо 0100101 было принято 0100111.

Для обнаружения ошибки производят уже знакомые нам проверки на чётность.

Первая проверка: сумма $\Pi_1+\Pi_3+\Pi_5+\Pi_7=0+0+1+1$ четна. В младший разряд номера ошибочной позиции запишем 0.

Вторая проверка: сумма $\Pi_2+\Pi_3+\Pi_6+\Pi_7=1+0+1+1$ нечетна. Во второй разряд номера ошибочной позиции запишем 1.

Третья проверка: сумма $\Pi_4+\Pi_5+\Pi_6+\Pi_7=0+1+1+1$ нечетна. В третий разряд номера ошибочной позиции запишем 1.

Получили двоичный номер ошибочной позиции: 110_2 или 6_{10}.

Следовательно, символ шестой позиции следует изменить на обратный, и получим правильную кодовую комбинацию.

Если номер ошибочно позиции равен нулю — при передаче кода не было допущено ошибок.

Отметим, что построенный код позволяет обнаружить и исправить только одиночную ошибку. Чтобы получить возможность обнаружения двойной ошибки можно увеличить длину кода на ещё контрольный символ, значение которого будет определяться из условия чётности суммы всех единиц в коде. Тогда, добавив на принимающей стороне ещё одну (аналогичную) проверку на чётность, можно будет исправить одиночную ошибку и обнаружить двойную.

Методические материалы к лабораторной работе по теме «Теория информации»

Задача 1

Получение любой информации, в том числе, и измерительной, теория информации трактует как устранение (возможно частичное) некоторой неопределённости. Одним из простейших способов измерения (оценки) некоторой величины является использование *порядковых шкал* (шкал порядка), строящихся на отношениях тождества и порядка. Измерение с использованием таких шкал даёт достаточно грубые результаты, т.к. разность между субъектами шкалы не учитывается. В случае измерения по шкалам порядка весь диапазон возможных значений измеряемой величины разбивается на ряд интервалов. Неопределённость до измерения характеризуется тем, что неизвестно, в каком из интервалов лежит значение измеряемой величины. Результатом измерения является указание того, что измеряемая величина лежит в данном интервале, что означает сужение области неопределённости, а, следовательно, её уменьшение. Таким образом, с точки зрения теории информации результат измерения заключается в выборе конкретного интервала из целого ряда возможных интервалов.

В качестве примеров ниже приведены три шкалы: шкала Бофорта для определения скорости ветра, шкала Мооса для оценки относительной твёрдости минералов и шкала Медведева — Шпонхойера — Карника для оценки интенсивности землетрясений.

Шкала Бофорта для оценки скорости ветра

Баллы	Название	Признаки	Скорость, м/с
0	Штиль	Дым поднимается вертикально	0–0,2
1	Тихий	Дым поднимается слегка наклонно	0,3–1,5
2	Легкий	Ветер ощущается, шелестят листья	1,6–3,3

3	Слабый	Развеваются флаги	3,4–5,4
4	Умеренный	Ветер поднимает пыль	5,5–7,9
5	Свежий	Качаются тонкие стволы деревьев	8,0–10,7
6	Сильный	Гудят провода	10,8–13,8
7	Крепкий	Качаются стволы деревьев	13,9–17,1
8	Очень крепкий	Трудно идти против ветра	17,2–20,7
9	Шторм	Ветер начинает разрушать крыши	20,8–24,4
10	Сильный шторм	Ветер вырывает деревья с корнем	24,5–28,4
11	Жестокий шторм	Большие разрушения	28,5–32,6
12	Ураган	Огромные разрушения	>32,6

Шкала Мооса для оценки относительной твёрдости

Твёрдость	Эталонный минерал	Обрабатываемость	Абсолютная твёрдость
1	Тальк	Царапается ногтем	1
2	Гипс	Царапается ногтем	3
3	Кальцит	Царапается медной монетой	9
4	Флюорит	Легко царапается ножом	21
5	Апатит	С усилием царапается ножом	48
6	Ортоклаз	Царапается напильником	72
7	Кварц	Поддаётся обработке алмазом	100
8	Топаз	Поддаётся обработке алмазом	200
9	Корунд	Поддаётся обработке алмазом	400
10	Алмаз	Режет стекло	1600

Шкала Медведева — Шпонхойера — Карника

Баллы	Сила землетрясения	Характеристика
I	Не ощущается	Отмечается только сейсмическими приборами
II	Очень слабые толчки	Ощущается чуткими домашними животными
III	Слабое	Ощущается как сотрясение от грузовика
IV	Интенсивное	Внутри здания ощущается большинством людей
V	Довольно сильное	Ощущается людьми и вне зданий
VI	Сильное	Ощущается всеми
VII	Очень сильное	Повреждения в стенах каменных домов
VIII	Разрушительное	Трещины на крутых склонах и на сырой почве
IX	Опустошительное	Сильное повреждение и разрушение домов
X	Уничтожающее	Трещины в почве иногда до метра шириной
XI	Катастрофа	Многочисленные оползни и обвалы
XII	Сильная катастрофа	Изменяется рельеф

Определить (предполагается, что вероятности попадания измеряемой величины в любой из интервалов равны между собой):

- число интервалов шкалы n_0 (возможное число состояний системы);
- число интервалов n (число состояний системы) после измерений;
- априорную (безусловную) энтропию H_0;
- апостериорную (условную) энтропию H;
- количество измерительной информации I.

Указание. Используемая шкала и интервал неопределенности после проведения измерений (в баллах соответствующей шкалы) приведены в таблице вариантов.

Порядок расчёта

Область неопределённости до измерения простирается на все интервалы шкалы, поэтому n_0 соответствует числу интервалов, на которые разбита шкала. Число интервалов n (после измерений) определяется согласно варианту. При условии, что вероятности попадания измеряемой величины в любой из интервалов равны между собой, неопределённость ситуации до и после измерений характеризуется энтропией, равной логарифму числа интервалов (состояний системы):

$H_0 = \log_2 n_0$, $H = \log_2 n$.

Количество измерительной информации I рассчитывается по формуле

$I = H_0 - H$.

Таблица вариантов

Варианты 1-10										
№ варианта	1	2	3	4	5	6	7	8	9	10
Шкала	Шкала Бофорта									
Результат измерения (в баллах)	от 0 до 3	от 5 до 6	10	от 5 до 7	от 4 до 8	0	от 9 до 12	от 1 до 3	от 5 до 9	от 10 до 11
Варианты 11-20										
№ варианта	11	12	13	14	15	16	17	18	19	20
Шкала	Шкала Мооса									
Результат измерения (в единицах твёрдости)	от 2 до 4	от 1 до 2	от 6 до 10	9	от 6 до 8	от 8 до 9	6	от 2 до 6	от 3 до 5	от 1 до 4
Варианты 21-30										
№ варианта	21	22	23	24	25	26	27	28	29	30
Шкала	Шкала Медведева — Шпонхойера — Карника									
Результат измерения (в баллах)	от II до III	XII	от IX до XI	от IV до VII	от III до VII	от IX до X	от VII до XI	от IV до VI	V	от II до V

Задача 2

Измерительная информация по интервальной шкале получается путём сравнения друг с другом двух размеров Q_i и Q_j (предполагается, что один из них известен, а другой требуется найти) одной физической величины (например, массы) с помощью *компаратора* (например, равноплечих весов). Результатом каждого отдельного сравнения (отсчёта) является одно из трёх выражений:

$Q_i > Q_j$, $Q_i = Q_j$, $Q_i < Q_j$,

т.е. решение о том, больше (меньше) или равен один размер другому.

Для повышения точности результатов измерения проводят многократно (n раз). В каждой серии из n отсчётов каждый из трех возможных результатов измерения ($Q_i > Q_j$, $Q_i = Q_j$, $Q_i < Q_j$) встречается m_k раз, где $k = 1,2,3$ (возможный результат $Q_i > Q_j$ встречается m_1 раз, возможный результат $Q_i = Q_j$ встречается m_2 раз, возможный результат $Q_i < Q_j$ встречается m_3 раз).

Рассчитать:

a) «частость» (вероятность) каждого из возможных результатов;

b) априорную (безусловную) энтропию H_0;

c) апостериорную (условную) энтропию H_n;

d) количество измерительной информации I_n в каждой серии.

Построить по расчетным данным графики:

a) зависимости апостериорной энтропии H_n от числа измерений n: $H_n = f(n)$;

b) зависимости количества информации I_n от числа измерений n: $I_n = f(n)$.

Указание. Вычисления ведутся для четырёх серий измерений.

Для вариантов с 1 по 15 в первой серии измерений $n = 10$, во второй серии $n = 20$, в третьей серии $n = 40$, и в четвертой серии $n = 80$.

Для вариантов с 16 по 30 в первой серии измерений $n = 15$, во второй серии $n = 30$, в третьей серии $n = 60$, и в четвертой серии $n = 100$.

Порядок расчёта

Для расчёта априорной энтропии используется формула

$$H_0 = -\sum_{k=1}^{3} p_k \log_2 p_k,$$

с учётом, что все три результата измерения равновероятны ($p_1 = p_2 = p_3 = 1/3$).

Расчёт апостериорной энтропии выполняется по формуле

$$H_n = -\sum_{k=1}^{3} p_{nk} \log_2 p_{nk},$$

где $p_{nk} = m_k / n$ — «частость» (вероятность) каждого результата в серии из n отсчётов.

Количество измерительной информации I_n, полученной в каждой серии, рассчитывается по формуле

$I_n = H_0 - H_n$.

Таблица вариантов

n	m_k	Варианты 1-15														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	m_1	8	1	1	7	1	1	6	2	2	5	3	2	4	3	3

	m_2	1	8	1	1	7	2	2	6	2	3	5	3	3	4	3
	m_3	1	1	8	2	2	7	2	2	6	2	2	5	3	3	4
20	m_1	18	1	1	17	1	2	16	2	2	15	2	3	14	2	4
	m_2	1	18	1	1	17	1	2	16	2	2	15	2	2	14	2
	m_3	1	1	18	2	2	17	2	2	16	3	3	15	4	4	14
40	m_1	38	1	1	37	1	1	36	1	2	34	2	4	33	4	3
	m_2	1	38	1	2	37	2	1	36	2	3	34	2	3	33	4
	m_3	1	1	38	1	2	37	3	3	36	3	4	34	4	3	33
80	m_1	78	1	1	77	1	2	76	3	1	75	3	4	74	3	2
	m_2	1	78	1	2	77	1	2	76	3	2	75	1	3	74	4
	m_3	1	1	78	1	2	77	2	1	76	3	2	75	3	3	74

n	m_k	Варианты 16-30														
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
15	m_1	13	1	1	12	2	2	11	1	3	10	4	2	9	2	4
	m_2	1	13	1	2	12	1	2	11	1	3	10	3	3	9	2
	m_3	1	1	13	1	1	12	2	3	11	2	1	10	3	4	9
30	m_1	28	1	1	27	1	1	26	3	2	25	1	3	24	4	2
	m_2	1	28	1	1	27	2	1	26	1	2	25	2	2	24	4
	m_3	1	1	28	2	2	27	3	1	26	3	4	25	4	2	24
60	m_1	58	1	1	57	2	2	56	2	1	55	3	1	54	5	3
	m_2	1	58	1	2	57	1	3	56	3	4	55	4	4	54	3
	m_3	1	1	58	1	1	57	1	2	56	1	2	55	2	1	54
100	m_1	98	1	1	97	1	1	96	2	2	95	2	4	94	3	5
	m_2	1	98	1	1	97	2	2	96	2	1	95	1	1	94	1
	m_3	1	1	98	2	2	97	2	2	96	4	3	95	5	3	94

Задача 3

Измерительная информация по абсолютной шкале (шкале отношений) получается с помощью аналогового прибора. При любом измерении обязательно используется априорная информация.

Априорной информацией может являться:

1. Интервал $[Q_1 \quad Q_2]$, в пределах которого находится значение измеряемой величины.
2. Закон распределения вероятности (ЗРВ) значений измеряемой величины в этом интервале.

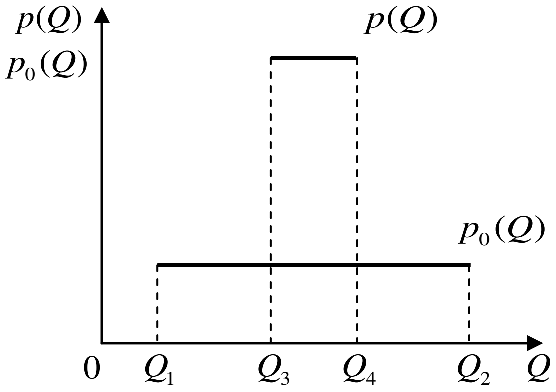
Если ЗРВ неизвестен, то его заменяют ситуационной моделью, в качестве которой чаще всего используют равномерный ЗРВ.

После измерения происходит уточнение значения измеряемой величины:

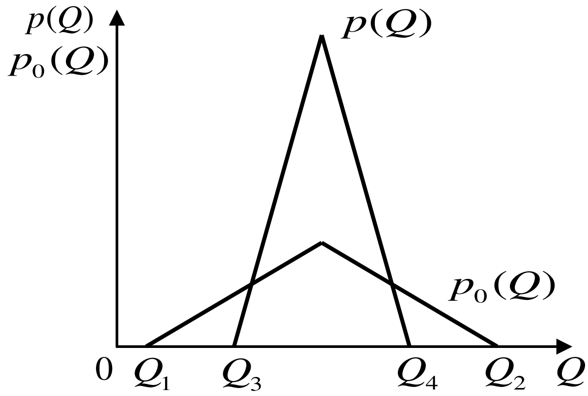
1. Меньше становится апостериорный интервал неопределенности $[Q_3 \quad Q_4]$ и уточняются параметры ЗРВ.
2. Становится известным ЗРВ, если он не был известен (при многократном измерении).

Некоторые законы распределения (и соответствующие им расчётные формулы) представлены в таблице в приложении.

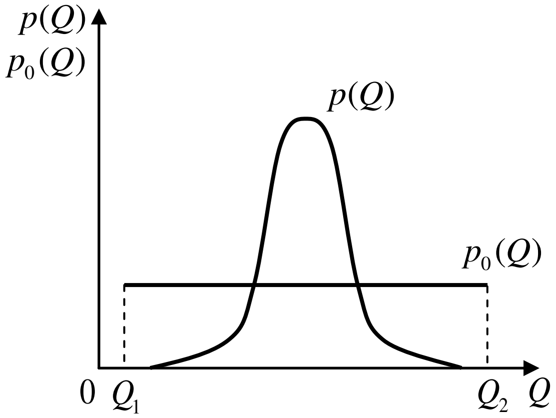
Для иллюстрации приведённых рассуждений на рис. 1 графически представлены четыре примера результатов экспериментов по измерению некоторой величины Q.



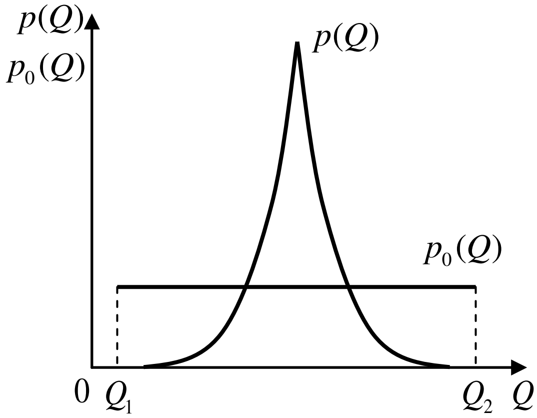
а) априорный ЗРВ — равномерный
апостериорный ЗРВ — равномерный



б) априорный ЗРВ — треугольный
апостериорный ЗРВ — треугольный



в) априорный ЗРВ — равномерный
апостериорный ЗРВ — нормальный



г) априорный ЗРВ — равномерный
апостериорный ЗРВ — экспоненциальный

Рис.1

На рис.1 рассмотренная информационная модель измерения представлена графически для следующих четырёх случаев:

1. Уменьшился интервал неопределенности значений измеряемой величины при известном равномерном ЗРВ.
2. Уменьшился интервал неопределенности значений измеряемой величины при известном треугольном ЗРВ.
3. Ситуационная модель (равномерный ЗРВ) после измерения заменена найденным из опыта нормальным ЗРВ.
4. Ситуационная модель (равномерный ЗРВ) после измерения заменена найденным из опыта экспоненциальным ЗРВ.

Рассчитать априорную (безусловную) энтропию H_0, апостериорную (условную) энтропию H и количество измерительной информации I для следующих трёх комбинаций априорного и апостериорного законов распределения информации:

Варианты	Эксперимент		
	№ 1	№ 2	№ 3
1	равномерный – равномерный	равномерный – нормальный	треугольный – экспоненциальный
2	равномерный – экспоненциальный	равномерный – равномерный	треугольный – нормальный
3	равномерный – треугольный	нормальный – нормальный	равномерный – экспоненциальный
4	треугольный – треугольный	экспоненциальный – экспоненциальный	равномерный – нормальный
5	нормальный – нормальный	треугольный – треугольный	равномерный –

Варианты	Эксперимент		
	№ 1	№ 2	№ 3
			экспоненциальный
6	треугольный – нормальный	треугольный – экспоненциальный	равномерный – треугольный
7	треугольный – равномерный	равномерный – экспоненциальный	нормальный – нормальный
8	треугольный – экспоненциальный	равномерный – равномерный	треугольный – нормальный
9	экспоненциальный – экспоненциальный	треугольный – нормальный	равномерный – равномерный
10	треугольный – треугольный	равномерный – экспоненциальный	треугольный – нормальный
11	треугольный – экспоненциальный	треугольный – треугольный	нормальный – нормальный
12	равномерный – нормальный	равномерный – треугольный	треугольный – треугольный
13	треугольный – экспоненциальный	треугольный – равномерный	равномерный – нормальный
14	равномерный – треугольный	треугольный – экспоненциальный	экспоненциальный – экспоненциальный
15	равномерный – нормальный	треугольный – нормальный	треугольный – экспоненциальный
16	равномерный – треугольный	нормальный – нормальный	равномерный – экспоненциальный
17	треугольный – равномерный	равномерный – экспоненциальный	нормальный – нормальный
18	экспоненциальный – экспоненциальный	треугольный – нормальный	равномерный – равномерный
19	равномерный – экспоненциальный	равномерный – равномерный	треугольный – нормальный
20	равномерный – нормальный	равномерный – треугольный	треугольный – треугольный
21	треугольный – треугольный	равномерный – экспоненциальный	треугольный – нормальный
22	равномерный – нормальный	треугольный – нормальный	треугольный – экспоненциальный
23	равномерный – равномерный	равномерный – нормальный	треугольный – экспоненциальный
24	треугольный – экспоненциальный	треугольный – равномерный	равномерный – нормальный
25	треугольный – треугольный	экспоненциальный – экспоненциальный	равномерный – нормальный
26	равномерный – треугольный	треугольный – экспоненциальный	экспоненциальный – экспоненциальный
27	треугольный – нормальный	треугольный – экспоненциальный	равномерный – треугольный
28	треугольный – экспоненциальный	равномерный – равномерный	треугольный – нормальный
29	треугольный – экспоненциальный	треугольный – треугольный	нормальный – нормальный
30	нормальный – нормальный	треугольный – треугольный	равномерный – экспоненциальный

Построить в выбранном масштабе априорные $p_0(Q)$ и апостериорные $p(Q)$ плотности распределения вероятности для всех трёх экспериментов согласно варианту аналогично тому, как это показано на рис. 1.

Указание. Исходные данные для расчета выбираются из таблицы в соответствии с вариантом.

Характеристики используемых ЗРВ приведены в справочной таблице.

Значение среднеквадратического отклонения σ дано для нормального и экспоненциального апостериорных законов распределения.

Порядок расчета

В справочной таблице приведены все необходимые данные. Для расчета априорной H_0 и апостериорной H энтропии воспользоваться формулами, приведенными в соответствующем столбце этой таблицы.

Количество измерительной информации рассчитывается по формуле

$I_n = H_0 - H$

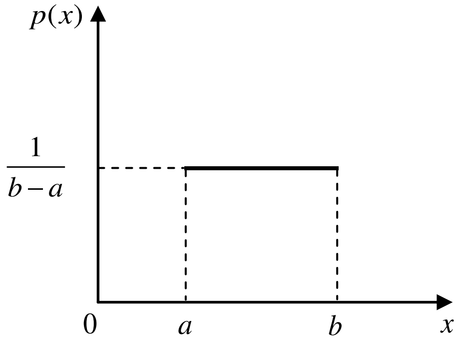
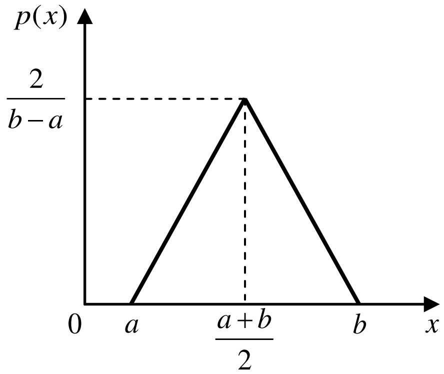
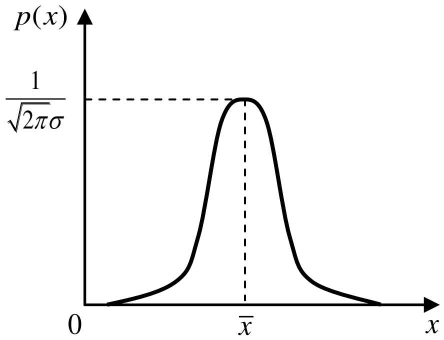
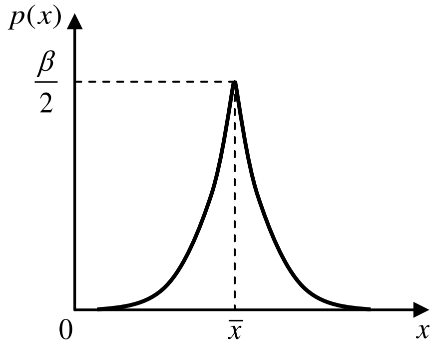
Для построения графиков плотности распределения вероятности $p_0(Q)$ и $p(Q)$ использовать формулы, приведенные справочной таблице.

Обратите внимание! Для нормального и экспоненциального законов распределения графики строятся по точкам в интервале $\left[\bar{Q}-3\sigma \quad \bar{Q}+3\sigma\right]$.
Числовые значения σ необходимо выбрать из таблицы в соответствии со своим вариантом (при использовании формул из справочной таблицы принять $Q=x$, $\overline{Q}=\bar{x}$).

Таблица вариантов

Параметры распределения	Варианты 1-15														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Q_1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Q_2	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Q_3	7	7	9	10	11	11	13	14	15	15	17	18	19	20	21
Q_4	9	11	11	12	13	15	15	16	17	19	19	20	21	22	23
σ	1	0.5	1.2	1.5	0.5	1	1.2	1.5	1.2	1.5	1	0.5	1.2	1	0.5
Параметры распределения	**Варианты 16-30**														
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Q_1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Q_2	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44
Q_3	8	10	12	13	16	18	19	22	24	25	28	30	31	34	36
Q_4	10	12	14	17	18	20	23	24	26	29	30	32	35	36	38
σ	1.2	1.5	1	0.5	0.7	1.2	0.5	1	1.2	1.5	0.5	1.7	1.5	1	0.5

Законы распределения

№	Закон распределения	Формула плотности вероятности	Энтропия
1	Равномерный 	$p(x)=\dfrac{1}{b-a}$ $a<x<b$	$H=\ln(b-a)$
2	Треугольный (Симпсона) 	$p(x)=\begin{cases}\dfrac{4(x-a)}{(b-a)^2}, & a<x<\dfrac{a+b}{2}\\ \dfrac{4(b-x)}{(b-a)^2}, & \dfrac{a+b}{2}<x<b\end{cases}$	$H=\ln\dfrac{(b-a)\sqrt{e}}{2}$
3	Нормальный (Гаусса) 	$p(x)=\dfrac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(x-\bar{x})^2}{2\sigma^2}}$	$H=\ln(\sigma\sqrt{2\pi e})$
4	Экспоненциальный двухсторонний (Лапласа) 	$p(x)=\dfrac{\beta}{2}e^{-\beta\lvert x-\bar{x}\rvert}$, $\beta=\dfrac{\sqrt{2}}{\sigma}$	$H=\ln\dfrac{2e}{\beta}=$ $=\ln(\sigma e\sqrt{2})$

Контрольные вопросы

1. Что изучает теория информации?
2. Какие существуют подходы к измерению информации?
3. Что такое энтропия источника информации?
4. Как связаны информация и энтропия?
5. Запишите формулы Хартли и Шеннона и укажите области их применения.

6. Какой из законов распределения вероятности (задание 3) используется чаще всего в качестве ситуационной модели? Почему?